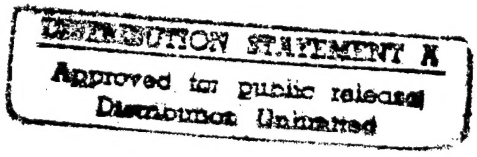
DATE: 4/02/97

CONTROLLING OFFICE FOR THIS DOCUMENT IS:
Commandant
Army Management Staff College (AMSC)
Fort Belvoir, VA 22060

POC: Commandant

DISTRIBUTION STATEMENT A: Public release



19970402 009

DTIC QUALITY INSPECTED 3

The Potential Impact of Dedicated Intelligence Internet Sites on the Role of US Army Counterintelligence as a Force Multiplier

Introduction

This paper proposes creating dedicated intelligence Internet web sites for Army strategic and tactical CI units. These sites will be accessible from anywhere in the world by Army intelligence personnel through designated Army core groups. The intent of this system is to create a common user data base for tactical and strategic CI Army elements, assist in the cross-training of tactical and strategic assets within the Army, and maximize resource capability to fulfill their force protection role. Within the next two years, other military departments will develop their intelligence networks and common data bases, which will be followed by national level intelligence agencies. The ultimate goal is to develop a data base, which will provide National Military Strategy (NMS) and National Security Strategy (NSS) leaders an evaluated product derived from information provided by the entire U.S. intelligence community. Such a system does not currently exist. Also suggested are several ways this kind of system could facilitate the training and mentoring of CI personnel stationed worldwide.

Within the context of this paper, counterintelligence (CI) is defined as "identifying, exploiting, and neutralizing a foreign intelligence service threat against Department of the Army personnel, equipment, facilities, and installations." Protection of these elements become a force multiplier for the warfighter. Today this role includes preventing technology transfer, which becomes a major force protection measure.

Impact of Downsizing and Absence of Common Data Bases

Downsizing has dramatically reduced the size of the strategic and tactical CI workforce in the Department of Defense, and, in particular, within the Army. To meet this challenge, the US Army is using current information technology to effectively husband its limited resources. Although there are numerous secure intelligence communications systems within the Army, information is compartmented and rarely shared with other units. Common accessible data bases are not widespread within the Army, much less within the US intelligence community at large. Duplication of effort within the US intelligence community does not markedly improve support to the NMS or the NSS. Creating the means to securely transmit and receive classified information from multiple users located around the world will result in a system capable of providing national leaders with a total product, not one developed from a single intelligence service.

If Army CI is to prepare for the 21st Century, it must begin using information technology now to understand its capabilities and potential applications. We must rapidly integrate technology "know-how" into all facets of CI, if we are to marshal our limited resources to fulfill mission needs.

The level of experience in many Army Military Intelligence Resident Office has been radically reduced as a consequence of the downsizing of the Army's CI workforce. In 1994, for example, there were 22 members assigned to the National Capital Region Resident

Office (NCRRO) at Fort Belvoir, Virginia. Today there are only three. According to Paul Godlewski, Special Agent in Charge of the NCRRO, he has 16 years of military service and the remaining two members have five years each. (Godlewski, 14 Nov 96) NCRRO is not an isolated example of the impact of downsizing within the Army's CI community. If CI is to contribute to force protection by the prevention of technology transfer, then innovative ways of using information technology must be created, explored, and, above-all, shared.

Intelligence personnel are beginning to routinely use available technologies to gather supporting information for investigative leads or to fulfill assigned functions, such as, preparing a Subversion and Espionage Directed Against the Army (SAEDA) briefing. For example, an effective SAEDA *unclassified* briefing can be developed by using the Internet to access the Country Study Fact Sheets produced by the Central Intelligence Agency (CIA) or the Department of State (DOS).

Unfortunately, successful ventures or accomplishments are generally not recognized by higher headquarters, and as a consequence, success stories are not disseminated throughout a core group command. Higher headquarters are interested in statistical results; not necessarily the methodology used to acquire the end product. This trend must be reversed if technology transfer is to be identified, tracked, and defeated by today's small Army CI contingent. Secure web sites will allow peers, friends, mentors to brainstorm the "how to" attack a problem. This aspect of the proposed system will energize critical thinking *throughout the entire system*, as opposed to relying on appointed leaders to resolve issues. This is a force multiplier in the purest sense.

We must advertise the "how we did it" to other investigators and intelligence operators, in order to augment experience lost due to downsizing. Shared knowledge of methodology used to advance an investigation or operation in today's technology driven environment is crucial in educating investigators and intelligence professionals, many of whom have not attended any formal professional training in years. Creating dedicated intelligence networks will assist in training, educating, and mentoring our workforce.

The System in General

The proposed intelligence network suggests information will be shared by using the Internet and will involve several dedicated network servers using modified software to protection data/information.

Three separate Internet webs will be used to tie several geographic core Army intelligence organizations together. One Internet will use INTELINK-S software dedicated to Secret collateral information, while the second classified World Wide Web (WWW) Internet using INTELINK software should be dedicated to SCI. In addition to current raw information, these classified Internets will enable personnel to obtain finished intelligence products. Unclassified material could have its own dedicated web site with assigned protocol for set for Secret information. This protection level is to protect discussions concerning methodology, etc., not the information itself.

Currently, the intelligence community is moving towards establishing a complete collateral Secret WWW, which will run on the Secret Internet Protocol Routing Network (SIPRNET) (Turner, Sep 96, pg 43). Within the next two years, plans envision four specific web sites being activated: Army, Air Force, Navy, and one for OSIA [On Sight Inspection Agency]. Over the next three or four years, national level organizations (CIA, FBI, and DIA) will be gradually added to the system. The overall goal is to establish a joint data base within the intelligence community capable of producing a holistic intelligence product in response to a national crisis, should the need arise.

According to Mark Deeds, Chief, Information Management Office, Foreign

Counterintelligence Activity, this Internet system will also benefit the Combatant Commanders, who will have access to the Secret and SCI nets, in order to monitor current information relating to his area(s) of concern. When the systems are established, users will be able to use web technology, like Yahoo, to search for information provided by other organizations within the intelligence community. It will also be possible to locate finished intelligence products authored by other intelligence agencies. (Deeds, 14 Nov 1996) Overall, this system will facilitate exchange of information and generate discussion between members of the US intelligence community, particularly between Army intelligence members involved in force protection.

Suggested core Army units for both classified systems are: 902d MIG and the 513th MI Bde in the US; 650th MIG and 66th MIG in Europe; and the 500th and 501st MI Brigades in the Far East. These units know what needs to be protected and the overall threats to security within their geographic area of responsibility. The dedicated net sites will 1) facilitate coordination and sharing of information and ideas from intelligence units world wide 2) allow users to freely discuss possible intelligence applications of information technology to on-going investigations or operations and 3) allow passage of information directly to interested customers. For example, a terrorist incident in Japan may be of interest to the CINC EUCOM and the 66th MIG in Germany, if the terrorist organization has a following in Germany.

Current WWW Internet Use Limitations

Agents are able to tailor requests for unclassified information through the judicious use of available commercial Internet websites. Access to classified data bases with evaluated intelligence is severely restricted largely due to the absence of an intelligence Internet with the requisite security measures to preclude compromise of holdings. Systems that do exist are not linked. The need to know principle when combined with the requirement to deal with individual intelligence agencies separately, does not create an environment for a timely response to most inquiries. Although you may submit a request for information through the "chain of command," the final product may not be received in time or be what you want. **A dedicated classified intelligence network** will eliminate this deficiency. *If Army* CI is to contribute to preventing technology transfer, access must be expanded from unclassified sources to evaluated information from joint sources.

An Example of the Current System

The following example illustrates what an experienced CI agent can develop using current commercially available WWW sites. The military net (MILNET), which contains unclassified information, can be accessed through the Internet to provide useful CI leads to prevent technology transfer. Using the MILNET to access the DTIC (Defense Technology Intelligence Center) data base allows an agent to conduct an electronic search for companies denied government contracts. Results of such inquires provide investigators with the types of information certain companies were attempting to acquire. Further electronic checks and coordination with other investigative agencies could ascertain that a certain foreign government was using retired military personnel and attempting to acquire technology denied by treaty or agreements.

In my example, the agent identified a threat to U.S. national security, one which could have impacted on a CINC. Equally important, is using the dedicated intelligence net to discuss methodology, tactics, and issues. Such actions would most likely generate a lively discussion of other successful investigative or operational methods used or raise "what if" scenarios. If we are to fully develop our capabilities with our reduced manpower levels, we must use information technology to our full advantage by sharing information with others in the community.

Currently, Army CI does not have a system to informally pass seemingly minor lessons learned information to others in the CI community. Investigative or operational results are entered into the appropriate channel without the higher headquarters learning how an individual agent successfully used information technology of today to do tomorrow's business smarter. Consequently, although we are doing "business smarter" in some circles, we need to do it better and on a broader scale. Establishing the multi-level internet web servers and sites help us accomplish this goal.

Perhaps the true potential benefit of the INTELINK systems concerns its use in seemingly unrelated roles. These systems will provide a unique opportunity to share with other CI units ground level experiences in leveraging information technology to accomplish assigned missions. For example, the use of the DTIC to identify investigative leads to thwart technology transfer. The INTELINK-S system can be used within the core groups to suggest operational, investigative, or tactical uses for off the shelf products in an operational/investigative or tactical role; OR use the system to access the "School Without Walls" at the US Army Intelligence Center and School (USAICS), Fort Huachuca, Arizona.

USAICS is actively developing Intelligence Training XXI strategy to promote several TRADOC 21st Century training initiatives: the evolution of Classroom XXI and "distance learning." (Turner, 96, pg 40) Classroom XXI is a concept which will reengineer the classroom of Army training institutions to capitalize on new training methods and leverage information technology. Once courses are designed, instructors will be able to rapidly up-date on-line lessons, thereby providing the most current doctrinal information to students. Moreover, courses of instruction can be reviewed by anyone with the appropriate pass word to determine MOS doctrine and methods.

As the School Without Walls and "distance learning" become established, it is entirely possible that interactive Internet courses will become common and can be applied to communicate with and train the force (active duty, reserve force and national guard structure) (MI Bulletin, Dec 95, pg 46). Interactive distance learning would certainly reduce the cost of training large numbers of personnel and has the distinct advantage of allowing distance learners to receive refresher training without travel being involved. For example, consider the writer of this paper. I attended the basic CI Agent Course nearly 28 years ago. Unquestionably, what I was taught then does not resemble what is taught now. Distance learning would enable me to take the course and to understand what training junior agents receive today. Based on this knowledge, I would know what skills and basic knowledge of CI procedures and doctrine to expect from a new agent and then could revise my training programs accordingly.

CONCLUSION: If US Army CI members are to meet the challenge of truly protecting the force, it must master and leverage information technology to the fullest extent possible. Developing a common intelligence data base will facilitate Army CI operations worldwide, particularly when Secret and SCI web sites and servers are established in the core Army groups. Within the next four or five years, the proposed system should include all military services and national level intelligence organizations. Developing investigative and operational skills today will place Army at the fore front in the fight against technology transfer. The system has a tremendous potential to facilitate training and mentoring of our workforce, and should be fully exploited to encourage critical thinking by all members.

Bibliography

Cairns, Donald W. The Doctrine Internet. INSCOM Journal Nov - Dec 95.

Deeds, Mark. Personal Interview. 8/19 Nov 96.

Fischer, Joan E. LIWA Levels Playing Field. INSCOM Journal May-Jun 95.

Godlewski, Paul. Personal Interview. 14 Nov 1996.

Humphreys, Vernon. Training the Total Organization. Training and Development Journal, Oct 90.

Hunter, Hal. The Opposite Sector. Training and Development Magazine, May 95.

Jones, Jerry. USAICS&FH. Personal Interview. 24 Oct 96.

Lowrey, Dennis A. Center Without Walls: Training in the Information Age. Military Intelligence Professional Bulletin, PB 34-95-4. Oct - Dec 95.

Juechter, W. Mather. Learning by Doing. Training and Development Magazine. Oct 93.

Turner, Edward F. School Without Walls: IEW Maintenance Training in the Information Age. MI Professional Bulletin. PB 34-96-3. Jul-Sep 96.

Ward, Edna C. and Lee, J. Edward. An Instructor's Guide to Distance Learning. Training and Development Magazine, Nov 95.

Back to Publications Page